Transport Layer Security (TLS) Lab

Xinyi Li

January 8, 2021

Instruction: https://seedsecuritylabs.org/Labs_20.04/Files/Crypto_TLS/Crypto_TLS.pdf

Lab Environment

Set up 3 containers:

```
client: 10.9.0.5
server: 10.9.0.43
proxy: 10.9.0.143
```

```
curl
    https://seedsecuritylabs.org/Labs_20.04/Files/Crypto_TLS/Labsetup.zip
    -o Labsetup.zip
unzip Labsetup.zip
cd Labsetup
dcbuild
dcup -d
```

Task 1

We try to create a TCP connection between our VM (**not container**) with https://github.com/

```
cd volumes
./handshake.py github.com
```

It gives:

```
After making TCP connection. Press any key to continue ...
=== Cipher used: ('TLS_AES_128_GCM_SHA256', 'TLSv1.3', 128)
=== Server hostname: github.com
=== Server certificate:
{'OCSP': ('http://ocsp.digicert.com',),
```

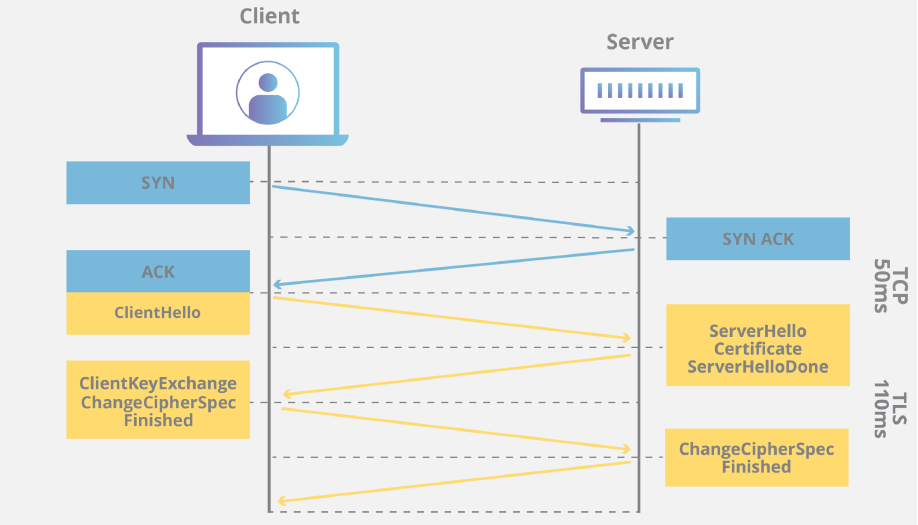
```
 'caIssuers':
    ('http://cacerts.digicert.com/DigiCertSHA2HighAssuranceServerCA.crt',),
 'crlDistributionPoints':
    ('http://crl3.digicert.com/sha2-ha-server-g6.crl',
                          'http://crl4.digicert.com/sha2-ha-server-g6.crl'),
 'issuer': ((('countryName', 'US'),),
            (('organizationName', 'DigiCert Inc'),),
            (('organizationalUnitName', 'www.digicert.com'),),
            (('commonName', 'DigiCert SHA2 High Assurance Server
                CA'),)),
 'notAfter': 'May 10 12:00:00 2022 GMT',
 'notBefore': 'May  5 00:00:00 2020 GMT',
 'serialNumber': '0557C80B282683A17B0A114493296B79',
 'subject': ((('countryName', 'US'),),
             (('stateOrProvinceName', 'California'),),
             (('localityName', 'San Francisco'),),
             (('organizationName', 'GitHub, Inc.'),),
             (('commonName', 'github.com'),)),
 'subjectAltName': (('DNS', 'github.com'), ('DNS',
    'www.github.com')),
 'version': 3}
[{'issuer': ((('countryName', 'US'),),
             (('organizationName', 'DigiCert Inc'),),
             (('organizationalUnitName', 'www.digicert.com'),),
             (('commonName', 'DigiCert High Assurance EV Root
                 CA'),)),
  'notAfter': 'Nov 10 00:00:00 2031 GMT',
  'notBefore': 'Nov 10 00:00:00 2006 GMT',
  'serialNumber': '02AC5C266A0B409B8F0B79F2AE462577',
  'subject': ((('countryName', 'US'),),
              (('organizationName', 'DigiCert Inc'),),
              (('organizationalUnitName', 'www.digicert.com'),),
              (('commonName', 'DigiCert High Assurance EV Root
                  CA'),)),
  'version': 3}]
```

Reference to the SSL module documentation, `/etc/ssl/certs/` specifies the location of CA certificates that are used to validate the servers' certificates.

It may be hard to keep tracing of packets in TLS handshake when running VNC server. So we can run the script in one container via `dockerps` and focus on the corresponding network interface:

No.	Time	Source	Destination	Protocol	Length	Info
1	2021-01-08 03:53:…	02:42:0a:09:00:05	Broadcast	ARP	42	Who has 10.9.0.1? Tell 10.9.0.5
2	2021-01-08 03:53:…	02:42:ad:33:28:82	02:42:0a:09:00:05	ARP	42	10.9.0.1 is at 02:42:ad:33:28:82
3	2021-01-08 03:53:…	10.9.0.5	168.63.129.16	DNS	70	Standard query 0x04a8 A github.com
4	2021-01-08 03:53:…	168.63.129.16	10.9.0.5	DNS	97	Standard query response 0x04a8 A github.com A 140.82.112.4 OPT
5	2021-01-08 03:53:…	10.9.0.5	140.82.112.4	TCP	74	41778 → 443 [SYN] Seq=633540107 Win=64240 Len=0 MSS=1460 SACK…
6	2021-01-08 03:53:…	140.82.112.4	10.9.0.5	TCP	74	443 → 41778 [SYN, ACK] Seq=3865109026 Ack=633540108 Win=65535…
7	2021-01-08 03:53:…	10.9.0.5	140.82.112.4	TCP	66	41778 → 443 [ACK] Seq=633540108 Ack=3865109027 Win=64256 Len=…
8	2021-01-08 03:53:…	140.82.112.4	10.9.0.5	TCP	74	[TCP Retransmission] 443 → 41778 [SYN, ACK] Seq=3865109026 Ac…
9	2021-01-08 03:53:…	10.9.0.5	140.82.112.4	TCP	66	[TCP Dup ACK 7#1] 41778 → 443 [ACK] Seq=633540108 Ack=3865109…
10	2021-01-08 03:53:…	10.9.0.5	140.82.112.4	TLSv1.3	583	Client Hello
11	2021-01-08 03:53:…	140.82.112.4	10.9.0.5	TLSv1.3	3573	Server Hello, Change Cipher Spec, Application Data, Applicati…
12	2021-01-08 03:53:…	10.9.0.5	140.82.112.4	TCP	66	41778 → 443 [ACK] Seq=633540625 Ack=3865112534 Win=62976 Len=…
13	2021-01-08 03:53:…	10.9.0.5	140.82.112.4	TLSv1.3	130	Change Cipher Spec, Application Data
14	2021-01-08 03:53:…	140.82.112.4	10.9.0.5	TLSv1.3	145	Application Data
15	2021-01-08 03:53:…	140.82.112.4	10.9.0.5	TLSv1.3	145	Application Data
16	2021-01-08 03:53:…	10.9.0.5	140.82.112.4	TCP	66	41778 → 443 [ACK] Seq=633540689 Ack=3865112613 Win=64128 Len=…
17	2021-01-08 03:53:…	10.9.0.5	140.82.112.4	TCP	66	41778 → 443 [ACK] Seq=633540689 Ack=3865112692 Win=64128 Len=…
18	2021-01-08 03:53:…	10.9.0.5	140.82.112.4	TCP	66	41778 → 443 [FIN, ACK] Seq=633540689 Ack=3865112692 Win=64128…
19	2021-01-08 03:53:…	10.9.0.5	140.82.112.4	TCP	66	41778 → 443 [RST, ACK] Seq=633540690 Ack=3865112692 Win=64128…
20	2021-01-08 03:53:…	02:42:ad:33:28:82	02:42:0a:09:00:05	ARP	42	Who has 10.9.0.5? Tell 10.9.0.1
21	2021-01-08 03:53:…	02:42:0a:09:00:05	02:42:ad:33:28:82	ARP	42	10.9.0.5 is at 02:42:0a:09:00:05

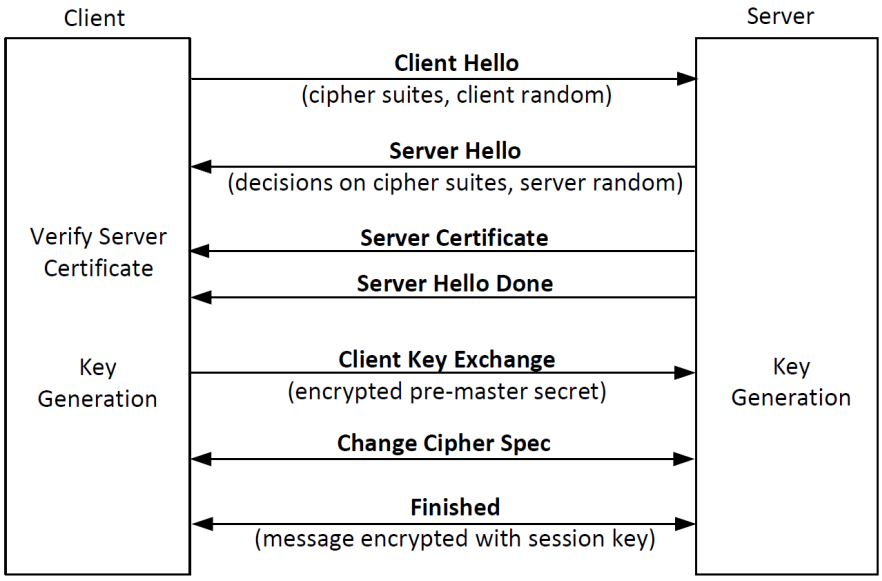
The captured packets depict a process as:



(the figure comes from https://www.cloudflare.com/learning/ssl/what-happens-in-a-tls-handshake/)

After a 3-way TCP handshake, a TCP connection is established (Line 23), the TLS handshake happens right after it (Line 29).

A clearer illustration of TLS handshake from the seed book:


Client
Server
Client Hello
(cipher suites, client random)
Server Hello
(decisions on cipher suites, server random)
Verify Server Certificate
Server Certificate
Server Hello Done
Key Generation
Client Key Exchange
(encrypted pre-master secret)
Key Generation
Change Cipher Spec
Finished
(message encrypted with session key)